ABSTRACT

Methods and apparatus are provided to monitor and analyze activity occurring on a networked computer system. In some embodiments, a method is provided for capturing, in a data structure, at least a portion of a notification describing a network event provided by a node on a computer network, identifying a data element (e.g., an IP address of the node) within the notification, and updating an index and/or summary based on the data element. The data structure may be stored in a file system maintained on a site, and sites may exchange information related to the notification data stored on each. In some embodiments, a query which is issued to a site may be processed using data transferred from other sites, and/or may be split into one or more additional queries which may be transmitted for processing to other sites.